Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2616

Vragen van de leden **Vuijk** en **Teeven** (beiden VVD) aan de Minister van Defensie over *gestolen data van Zwitserse speciale eenheden door Russische hackers* (ingezonden 10 mei 2016).

Antwoord van Minister **Hennis-Plasschaert** (Defensie) (ontvangen 24 mei 2016).

Vraag 1
Bent u bekend met het bericht «Russische Hacker enttarnen geheime Schweizer Elite-Truppe»?[1]

Antwoord 1
Ja.

Vraag 2
Klopt het dat geheime data van Zwitserse speciale eenheden is gestolen bij een cyberaanval door Russische hackers? Klopt het ook dat zij hierdoor een nieuwe identiteit verstrekt moeten krijgen? Graag een toelichting.

Antwoord 2
In reactie op de publicaties in de Zwitserse pers heeft het Zwitserse Ministerie van Defensie laten weten onderzoek te doen naar de cyberaanval en de mogelijke consequenties. Ook de vraag of leden van de Zwitserse speciale eenheid Aufklärungsdetachements 10 (AAD 10) een nieuwe identiteit verstrekt moeten krijgen, maakt onderdeel uit van het onderzoek.

Vraag 3
Hoe beoordeelt u de risico's van dergelijke cyberaanvallen voor de Nederlandse krijgsmacht, specifiek in het licht van waarschuwingen die de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) doet over cyberaanvallen, onder andere in haar meest recente jaarrapport? Is de Nederlandse krijgsmacht voldoende in staat zichzelf hier tegen te beveiligen en verdedigen? Graag een toelichting.

[1] Blick.ch, 8 mei 2016

ah-tk-20152016-2616
ISSN 0921 - 7398
's-Gravenhage 2016

Antwoord 3
De dreiging van digitale spionage tegen Defensie, toeleveranciers, bondgenootschappelijke netwerken en producenten van militair-relevante producten is aanzienlijk. Deze dreiging neemt in omvang toe en wordt steeds agressiever en geavanceerder. Defensie slaat dagelijks aanvallen af en er zijn vooralsnog geen cyberaanvallen bekend waarbij gevoelige informatie is buitgemaakt. Ondanks alle maatregelen is de voortdurende versterking van de digitale weerbaarheid geboden. Deze versterking maakt deel uit van de Defensie Cyber Strategie (Kamerstuk 33 321, nr. 5 van 23 februari 2015).
De maatregelen om de eigen informatietechnologie-systemen (IT-systemen) veilig te houden, maken deel uit van de diensten en producten die het Joint IV Commando (JIVC), waaronder het Defensie *Computer Emergency Response Team* (DefCERT), en de directie *Operations* van de Defensie Materieel Organisatie leveren. Defensie ontwikkelt doorlopend nieuwe beveiligingsmethodieken om nieuwe dreigingen (vroegtijdig) te kunnen onderkennen en af te slaan.

Vraag 4
Is specifiek de identiteit van zowel speciale eenheden als inlichtingenpersoneel van de Nederlandse krijgsmacht voldoende geborgd tegen cyberaanvallen? Is dit geval in Zwitserland reden voor Defensie om extra maatregelen te nemen? Graag een toelichting.

Antwoord 4
In haar meest recente jaarverslag (Kamerstuk 33 321, nr. 7 van 15 maart 2016) gaat de MIVD uitgebreid in op de verschillende dreigingen tegen Defensie in of via het cyberdomein. Spionageactiviteiten van statelijke actoren maken hier nadrukkelijk onderdeel van uit. Defensie doet er om deze reden alles aan om de vertrouwelijke informatie te beschermen. Over onder andere dit onderwerp heb ik de Tweede Kamer geïnformeerd in de voortgangsrapportage (Kamerstuk 33 321, nr. 7 van 15 maart 2016) over de uitvoering van de Defensie Cyber Strategie. De cyberaanval in Zwitserland past, ondanks de ernst van het incident, in het bestaande dreigingsbeeld en is om deze reden geen aanleiding om aanvullende maatregelen te nemen.

Vraag 5
Zijn er ooit pogingen gedaan door hackers om dergelijke data van Nederlandse eenheden te stelen? Zo ja, vanuit welke landen kwamen die cyberaanvallen en is bij dergelijke aanvallen ooit gevoelige informatie buitgemaakt? Op welke wijze is hierop gereageerd door Defensie?

Antwoord 5
Zie het antwoord op vraag 3.